UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/004,340	10/25/2001	Gavin A. McLintock	34118	4956

116 7590 02/03/2006

PEARNE & GORDON LLP
1801 EAST 9TH STREET
SUITE 1200
CLEVELAND, OH 44114-3108

EXAMINER	
TRUONG, LAN DAI T	
ART UNIT	PAPER NUMBER
2143	

DATE MAILED: 02/03/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 10/004,340	Applicant(s) MCLINTOCK ET AL.	
	Examiner lan dai thi truong	Art Unit 2143	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *03* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 January 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1 and 4-47* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1 and 4-47* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

1. This action is response to communications: amendment filed 01/06/2006. Claims 1-47 are pending. Claim 1, 4, 6-20, 23-25, Claims 2-3 are canceled. Claims 28-47 are added as new claims by applicant.

2. The applicant's argument file on 06/23/2005 have fully considered. Applicant's arguments are persuasive.

Claim rejections-35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or descrybed as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

1) Claims 1, 4-5, 8, 10, 13, 15-18, 20, 28-32, 35-36, 39- 44 and 46, are rejected under 35 U.S.C 103(a) as being un-patentable over Martin et al. (U.S 5,979,754), in view of Varma (U.S. 5,850,753)

In referring to claim 1, which is exemplary with claims 29 and 35-36, 39-40, 44, 46:

Martin discloses the invention substantially as claimed, including a system, which can be implemented in a computer hardware or software code for administering access to one or more doors comprising:

(a) A module for managing access privilege of one or more individuals for each door and assigning access authorization to each individual for the door: (Martin discloses a door control apparatus utilized a control system includes a computer for store and process data. The computer programmed implements to store the identity of all doors and rooms requiring the control in a given facility. The program will also include an identification of all individuals authorized to have entry to all or specific room of the facility and can associate a specific entry card with each room and each authorized person: column 3, lines 42-57; column 4, lines 66-67; column 5, lines 1-32

(b) A door database for storing a door identification uniquely assigned to each door and information on each authorized individual for each door: (Martin discloses the computer stores a key unique to each of the users, for stores an identification code unique to each of the doors. It assigns access authorization to at least one user for each door: column 3, lines 42-57; column 4, lines 66-67; column 5, lines 1-32; column 9, lines 35-44)

(c) A module for changing data stored in the door database: (Martin discloses when guest room check out, the computer will delete the guest personal information from the database: column 7, lines 30-44)

A door control/lock assembly mount on each door, the door control/lock assembly: (Martin discloses "entry card reader" which is equivalent to "door lock/control" is positioned adjacent each guest room door. Martin discloses that when the guest runs the proper "credit card" which is equivalent to "room key" through his/her guest room card reader, a door lock release apparatus at the guest room door will open the lock, this process is shared identical functionality with the limitation "A door lock/control assembly mounted on each door for reading the key presented by the user, for verifying that the key has access authorization, and for operating the door in response to the authorization for access." Furthermore, Martin discloses a method of using paging transmitters and paging receivers to transmit information from a central control system to individual door control units located at each controlled door. If the "computer" which is equivalent to "door/key administering system" recognizes and accepts that guest card as an approved key, then computer generates a signal which is sent to the door transceiver causing the lock to open to an "approved card" which is equivalent to " room key." Martin's door control system meets the limitation "The door lock/control assembly being communicatively connected to the door/key administering system via the communications network:" column 6, lines 6-67; column 4, lines 4-45; column 3, lines 47-55; column 4, lines 9-22; column 5, lines 1-32)

The door control/lock assembly, the door administering system and the key administering system communicating with each other through a communication network, the door control/lock assembly for identifying a user key when it is presented by a user, and for operating the door based on the access privilege of the user when the identified key of the user is the key of a key owner who is an authorized individual having access authorization to the door: (Martin discloses "guest's credit card" is equal to "unique key" for the assigned room. When the guest runs the proper credit card through his/her guest room card reader, a door lock release apparatus at the guest room door will open the lock: column 3, lines 47-55, column 4, lines 15-16)

However, Martin does not explicitly teach a key administering system for administering one or more keys separately from the administration of the access to the door, each key being uniquely assigned to a key owner, the key administering system having: a key database for storing one or more keys for each key owner, and a module for changing data stored in the key database

However, Varma discloses “a card reader” which is equivalent to “a key administering system” can be updated by itself with “a new access code” which is equivalent to “a key.” When the guest departures, the hotel cleaning staff changes the guest access code from card reader. The computer at front desk is physically separated with card reader and updated the new access code, see (Varma: column 1, lines 31-59)

Thus, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Varma’s ideas of the hotel staff changes access code for card reader with Martin’s system in order to provide separated operation system those either can update guest access code , see (Varma: column 1, lines 31-59)

In referring to claim 20 which is exemplary with claim 46:

Martin discloses the invention substantially as claimed, including a method, which can be implemented in a computer hardware or software code for administering access to one or more doors comprising:

At the door server, administering access to one or more doors, including:

Managing access privilege of one or more individuals for each door and assigning access authorization to each individual for the door; At a door database, storing a door identification uniquely assigned to each door and information on each authorized individual for each door, data stored in the door database being updatable: (Martin discloses “the computer” which is shared functionality with “door database” which stores the identity of all doors and rooms requiring control in a given facility, and identification of all individuals authorized to have entry to all or specific rooms of the facility and can associate a “specific entry card” which is equivalent to "room key" with each room and each authorized person: column 3, lines 42-57; column 4,lines 22-45; column 5, lines 1-30; column 7, lines 30-44)

At a door control/lock assembly, identifying a user key presented by a user: comparing the identified key to the keys of the key owner and verifying that the identified key is a key of a key owner who is an authorized individual having access authorization to the door; and operating the door based on the access privilege of the individual: (Martin discloses "entry card reader" which is equivalent to "door lock/control" is positioned adjacent each guest room door. Martin discloses that when the guest runs the proper "credit card" which is equivalent to "room key" through his/her guest room card reader, a door lock release apparatus at the guest room door will open the lock, this process is shared identical functionality with the limitation "A door lock/control assembly mounted on each door for reading the key presented by the user, for verifying that the key has access authorization, and for operating the door in response to the authorization for access." Furthermore, Martin discloses a method of using paging transmitters and paging receivers to transmit information from a central control system to individual door control units located at each controlled door. The computer recognizes and accepts that guest card as an approved key, then computer generates a signal which is sent to the door transceiver causing the lock to open to an "approved card" which is equivalent to " owner key:" column 6, lines 6-67; column 4, lines 4-45; column 3, lines 47-55; column 4, lines 9-22; column 5, lines 1-32)

However, Martin does not explicitly disclose at a key server, administering one or more keys separately from the administration of the access to the door, each key uniquely assigned to a key owner; and the authorization step is carried out through the communications network between the door server and the key server;

However, Varma discloses the communication between "a card reader" which is equivalent to "a key administering system" and "the computer at front desk" which is equivalent to "the administration of the access to the door" to operate for door opening; wherein the computer at front desk assigns the guest's assess code used for authorization to operate the door, see (Varma: column 1, lines 31-59)

Thus, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Varma's ideas of the hotel staff changes access code for card reader with Martin's system in order to provide separated operation system those either can update guest access code, see (Varma: column 1, lines 31-59)

<u>In referring to claim 4, the limitation:</u>

In addition to rejection in claim 1, Martin- Varma further discloses wherein the door control/lock assembly carries out the authorization process when the communication between the door control/lock assembly and the door and key administering system is interrupted: (Martin discloses that after the guest runs the "proper credit card" is "room key" through "his/her guest room card reader" which is equal to "door control/lock assembly", the "computer" which is equal to "door administering system" recognizes and accepts that the guest card as an approved key, then a signal is transmitted to the door transceiver causing the lock to open to an approved card: column 4, lines 21-45, 62-67; column 7, lines 30-44)

In referring to claims 5 and 24, the limitation:

In addition to rejection in claims 1 and 20, Martin- Varma further discloses wherein the communications network includes wireless communications network: (Martin discloses a door control apparatus useable in buildings or other facilities having many locked doors or rooms and requiring controlled access to the room. Martin discloses the method of using wireless communication to transfer information between the "computer" which is equivalent to "door/key administering system" located lock control center and guest room card reader located at guest room: abstract: lines 1-17; column 3, lines 62-67; column 4, lines 9-22, 58-62)

In referring to claims 8, 16, 32:

In addition to rejection in claims 1, 30 Martin- Varma further discloses wherein the key includes a key of the key owner includes signature unique to the respective key owner which is not unique to the door and recognizable by the door control/lock assembly: (Martin discloses that "the credit card is a key for the assigned room" which represents "key owner." Martin discloses when the guest runs the proper credit card through his guest "room card reader" which is equal to "door control/lock assembly", then door lock release apparatus at the guest room door will open the lock: column 3, lines 44-56; column 4, lines 15-16)

In referring to claim 10, the limitation:

In addition to rejection in claim 1, Martin- Varma further discloses an identification device for reading the user's key presented by the users of the key: (Martin discloses a guest room "credit card reader" which is equal to "an identification device" for reading the "credit card" which is equivalent to "room key" presented by the users: column 3, lines 44-56)

A lock adapted to be operated in response to the authorization from the door and key administering system; an embedded controller for controlling the operation of the identification device and the lock, and the authorization process: (Martin discloses if the "computer" which is equivalent to "door/key administering system" that is located at a central control center recognizes and accepts that guest card as an approved card, then the computer generates a signal which is sent to door transceiver causing the lock to open to an "approved card" which is equivalent to "room key: column 4, lines 1-45, 65-67; column 5, lines 1-30)

<u>In referring to claim 13, the limitation:</u>

In addition to rejection in claim 5, Martin- Varma further discloses wherein the door control/lock assembly further includes a wireless transmitter/receiver: (Martin disclosed method of using wireless communication between transmitter and guest room door wireless receivers: column 4, lines 1-67; column 5, lines 1-30)

<u>In referring to claim 15, the limitation:</u>

In addition to rejection in claim 10, Martin- Varma further discloses wherein the embedded controller includes a database for storing information on the keys and users such that, when the communication between the door assembly and the door and key administering system is interrupted. The door control/lock assembly can carry out the authorization process for the door associated therewith: (Martin discloses "computer" which is equivalent to "database" for storing information on “the guest’s credit cards” which is equivalent to “room keys”, identity of all doors and rooms requiring control in given facility, and identification of all individuals authorized to have entry to all or specific rooms of facility and can associate a “specific card” which is equal to “room key” with each room and each authorized person. Martin also discloses when the guest runs the proper credit card through his/her guest room card reader, if the computer which be located at central control center recognizes and accepts that “guest card” as an “approved key” then computer generates a signal which is sent to the door transceiver causing the lock to open to an “approved card” which is equivalent to “room key:” abstract, lines 6-12; column 3, lines 42-57; column 5, lines 1-32; column 4, lines 21-45, 62-67; column 7, lines 30-44)

<u>In referring to claim 17, the limitation:</u>

Martin- Varma discloses the invention substantially as disclosed in claim 1, further teach wherein the door administering system is physically separated from the key administering system

However, Varma discloses “the computer as front desk” is equivalent to “the door administering system” and “card reader” is equivalent to “the key administering system”, see (Varma: column 1, lines 31-39)

Thus, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Varma’s ideas of the hotel staff changes access code for card reader with Martin’s system in order to provide separated operation system those either can update guest access code, see (Varma: column 1, lines 31-59)

In referring to claim 18, the limitation:

In addition to rejection in claim 1, Martin- Varma further discloses wherein the stored data pertaining to the keys and the doors can be updated when required by a door administrator and stored data pertaining to the keys can be updated when required by a key administrator: (Martin discloses a "control system" which is equivalent to "the guest registration system" includes a computer programmed to include the identity of all doors, rooms and a list of "specific entry card" is equivalent to "room key" with each room and each authorized person. Martin discloses the guest registration system will assign the guest an available room, and "store" is equal to "update" the credit card identity information as a key for assigned room. Then upon check-out from the place of lodging, the computer simply "removes" is equal to "updates" the credit card identity information from the memory and cared ceases to function as a guest room key, this process is shared functionality with the limitation "the stored data pertaining to the keys and the doors can be updated when required:" column 3, lines 42-49; column 4, lines 66-67; column 5, lines 1-11; column 7, lines 30-44)

In referring to claim 28:

Martin- Varma discloses the invention substantially as disclosed in claim 1, further teachs wherein the key owner of a key is capable of changing the key of that key owner at the key database

Varma discloses when the guest departures, the hotel cleaning staff changes the guest access code from card reader, then the computer updates the new access code to provide to next guest, see (Varma: column 1, lines 31-59)

Thus, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Varma's ideas of the hotel staff changes access code for card reader with Martin's system in order to provide separated operation system those either can update guest access code, see (Varma: column 1, lines 31-59)

<u>In referring to claims 30-31:</u>

Martin- Varma discloses the invention substantially as disclosed in claim 1, further includes wherein the door administering system is administered by one or more door administrator: Martin discloses a "the computer" which represented of "door administering system" which stores the identity of all doors and rooms requiring control in a given facility, and identification of all individuals authorized to have entry to all or specific rooms of the facility and can associate a specific entry card with each room and each authorized person: column 3, lines 42-57, lines 62-67; column 4, lines 1-45; column 5, lines 1-32)

The key administering system is administered by one or more key administrators: (Varma "card reader" is administrated by staff or helpdesk, see (Varma: column 1, lines 31-59)

Thus, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Varma's ideas of the hotel staff changes access code for card reader with Martin's system in order to provide separated operation system those either can update guest access code, see (Varma: column 1, lines 31-59)

<u>In referring to claims 41-43:</u>

Martin- Varma discloses the invention substantially as disclosed in claim 1, further includes wherein the system gathers information includes: time of attempt to access a door, and identification of user who attempted the access, and information on attempts to gain access to the door by an unknown individual: (column 1, lines 21-34; column 2, lines 55-65)

2) Claim 9 is rejected under 35 U.S.C 103(a) as being un-patentable over Martin-Varma in view of Flick (U.S 6,130,606)

In referring to claim 9:

Martin - Varma discloses the invention substantially as disclosed in claim 1, but does not explicitly teach wherein the communication and authorization process between the door and key administering system and door control/clock assembly are carried out in a form of encrypted signals or message

However, Flick discloses a vehicle security system includes a controller may alternately generates door lock and un-lock commands responsive to the remote transmitter. Flick discloses the security system simply ignores signals other than properly encrypted signals from the remote transmitter, see (Flick: abstract, lines 1, 14-15; column 1, lines 64-67; column 2, lines 1-7).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify "wireless information signals" of Martin- Varma to "encrypted signals" that are sent from remote transmitter to receiver which is connected to microprocessor of vehicle security system as taught in Flick. The combination would have been obvious because on of ordinary skill in the art would have been motivated to deter vehicle theft see (Flick; column 1, lines 24-25).

3) Claims 14 and 45 are rejected under 35 U.S.C 103(a) as being un-patentable over Martin-Varma in view of Dunhame et al. (U.S 5,541,585)

In referring to claim 14, which is exemplary with claim 45:

Martin - Varma discloses the invention substantially as disclosed in claims 1 and 36, but does not explicitly teach wherein the door control/lock assembly further includes a module for assisting in the operation of the door control/lock assembly and sensing the status of the door, the assisting and sensing module including one or more of the following: a door open sensor, a speaker and microphone assembly, a camera, an activity fight, a buzzer, a call button, a battery condition sensor, a smoke sensor, a temperature sensor

However Dunhame discloses a security system for controlling building access that includes door open sensor, speaker and microphone, "dim light" which is equivalent to "activity light" and camera, see (Dunhame: column 5, lines 14-48; column 6, lines 51; column 7, lines 28-29).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify "guest room door" of Martin-Varma to "controlled portal such as door" which has mechanisms for securing the door such as door open sensor, speaker and microphone, "dim light" which is equivalent to "activity light" and camera as taught by Dunhame. The combination would have been obvious because on of ordinary skill in the art would have been motivated to control access of persons through a controlled door (Dunhame: abstract, lines 1-4).

4) Claim 25 are rejected under 35 U.S.C 103(a) as being un-patentable over Varma (U.S. 5,850,753) in view of Bengtsson et al. (U.S. 6,356,942)

In referring to claim 25:

Varma discloses the system architecture for controlling door includes “front desk computer” which assigns accessed code for the guest. The authorization for opening the door throughout based on the accessed code: (column 1, lines 25-41)

However, Varma does not explicitly discloses a Meta server being adapted to serve an address reference among the door administering system and the key manager systems

Bengtsson discloses “a server” which is equivalent to “a meta server” being adapted to service as an address reference for communication between peripheral devices: (abstract, lines figure 1D; column 9, lines 1-67; column 10, lines 1-67)

Thus, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Bengtsson’s ideas of using a server being serviced as an address reference with Varma’s system in order to speed up communication process.

5) Claims 11-12, 21-22 are rejected under 35 U.S.C 103(a) as being un-patentable over Martin-Varma, and further in view of Yulkowski (U.S 6,049,287)

In referring to claims 11 and 22, the limitation:

Martin - Varma discloses the invention substantially as disclosed in claims 1 and 20, but does not explicitly teach wherein each key owner has one or more keys for the door, and the door control/lock assembly includes two or more identification devices which are different from each other

However Yulkowski discloses a door system with electrical components associated therewith for sensing and reacting to emergency conditions. In this invention, Yulkowski discloses a controller may be an access control device has both a “keypad and card reader” those are equivalent to “identification devices”. Yulkowski taught that the card reader may be used to insert or slide a card to unlock or lock door, and the key-pad allows the input of an identification code to controller to allow the door to unlock or lock, see (Yulkowski: column 4, lines 59-67).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify "door control unit" of Martin-Varma to "door controller" may be an access control device as a key-pad and a card reader, wherein key-pad allows the input of identification code and card reader to insert or slide a card therethrough to unlock or lock the door is taught in Yulkowski. The combination would have been obvious because on of ordinary skill in the art would have been motivated to provide various degrees of security (Yulkowski: column 5, lines 1-4).

In referring to claim 12, the limitation:

Martin - Varma –Yulkowski discloses the invention substantially as disclosed in claim 11, and further discloses wherein the key owner is authorized for access to the door by using all or several of the keys

Yulkowski discloses a controller may be an access control device has both "keypad and card reader" those are equivalent to "identification devices". Yulkowski taught that the card reader and the keypad may intersect so that both a card and an identification code are required to gain access within an opening, see (Yulkowski: column 4, lines 59-67).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify "door control unit" of Martin - Varma to "door controller" so that both a card identification and an identification code are required to gain access within an opening as taught in Yulkowski. The combination would have been obvious because on of ordinary skill in the art would have been motivated to provide various degrees of security (Yulkowski: column 5, lines 1-4).

In referring to claim 21, the limitation:

Martin - Varma discloses the invention substantially as disclosed in claim 20, but does not explicitly teach storing two or more different unique key signatures for the user whereby all of the different key signatures are required to gain access to the door" is not disclosed by Martin

However Yulkowski discloses a controller may be an access control device has both "keypad and card reader" those are equivalent to "identification devices", that means each identification device must has predetermined key signature for the user. Yulkowski taught that card reader and keypad may intersect so that both a card and an identification code are required to gain access within an opening, see (Yulkowski: column 4, lines 59-67).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify "door control unit" of Martin - Varma to "door controller" so that both a card identification and an identification code are required to gain access within an opening as taught in Yulkowski. The combination would have been obvious because on of ordinary skill in the art would have been motivated to provide various degrees of security (Yulkowski: column 5, lines 1-4).

6) Claims 6-7, 19, 23 are rejected under 35 U.S.C 103(a) as being un-patentable over Martin-Varma in view of Kalajan (U.S 6,006,258)

In referring to claims 6, 23:

Martin- Varma discloses the invention substantially as disclosed in claims 1 and 20, further includes wherein the door/key administering system includes a door/key administering server system" is matched: (Martin discloses a control system which may be located at a central control center, this system includes a "computer" is equivalent to "door/key administering server" that stores identity of rooms and doors and "associated credit cards" which is equivalent to "room keys": column 3, lines 44-49; column 4, lines 66-67; column 5, lines –32; column 7, lines 30-44)

But Martin-Varma does not disclose the communications network includes an Internet Protocol communication.

However Kalajan discloses method of remote access destination network resources through transport protocols, see (Kalajan: column 3, lines 5-27). Kalajan's method meets the limitation "wherein the communications network includes an IP (Internet Protocol) communications network."

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify "computer" of Martin- Varma to "server" which is remotely access through an Internet protocol by client or employee as taught in Kalajan. The combination would have been obvious because on of ordinary skill in the art would have been motivated to remotely access destination network resources through Internet protocols, see (Kalajan: column 3, lines 5-27).

In referring to claims 7, 19 the limitation:

Martin - Varma discloses the invention substantially as disclosed in claims 1 and 6, but does not explicitly teach wherein the door control/lock assembly and the door and key administering server system are adapted to be controlled via a web browser operatively connected to the IP communications network" does not disclose by Martin

However, Kalajan discloses an employee can access "server" which is equivalent to "door/key administering server" by using a web browser through IP network, see (Kalajan: column 3, lines 50-67). Kalajan's method meets the limitation "Wherein the door control/lock assembly and the door/key administering server system are adapted to be controlled via a web browser operatively connected to the IP communications network."

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify "computer" of Martin - Varma to "server" which is remotely access through an Internet protocol by client or employee as taught in Kalajan. The combination would have been obvious because on of ordinary skill in the art would have been motivated to remotely access destination network resources through Internet protocols, see (Kalajan: column 3, lines 5-27).

7) Claim 26 is rejected under 35 U.S.C 103(a) as being un-patentable over Varma-Bengtsson in view of Kalajan (U.S 6,006,258)

In referring to claim 26:

Varma- Bengtsson discloses the invention substantially as disclosed in claim 25, but Varma does not disclose the communications network includes an Internet Protocol communication.

However Kalajan discloses method of remote access destination network resources through transport protocols, see (Kalajan: column 3, lines 5-27).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify "computer" of Varma- Bengtsson to "server" which is remotely access through an Internet protocol by client or employee as taught in Kalajan. The combination would have been obvious because on of ordinary skill in the art would have been motivated to remotely access destination network resources through Internet protocols, see (Kalajan: column 3, lines 5-27).

8) Claim 27 is rejected under 35 U.S.C 103(a) as being un-patentable over Varma-Bengtsson in view of Paxhia et al. (U.S U.S. 2002/0052935)

In referring to claim 27:

Varma- Bengtsson discloses the invention substantially as disclosed in claim 25, but Varma does not disclose wherein the Meta server is adapted to be controlled via web browser communicatively and operatively connected to Meta server through the communication network

However Paxhia discloses configuration and administration form-Netscape: (figure 12)

Thus, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Paxhia's ideas of using configuration and administration form-nestcape with Varma- Bengtsson's system in order to convenience server for the user.

9) Claims 37-38 are rejected under 35 U.S.C 103(a) as being un-patentable over Martin-Varma in view of Saliga (U.S 5,397,884)

In referring to claims 37-38:

Martin-Varma discloses the invention substantially as disclosed in claim 36, but does not explicitly disclose wherein the security settings includes a setting specifying who is authorized at specific times to the door

However, Saliga discloses method of setting a predetermined authorization time period, see (Saliga: column 2, lines 60-67; column 3, lines 1-50)

Thus, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Saliga's ideas of the hotel staff changes access code for card reader with Martin- Varma's system in order to set the predetermined authorization time period for door opening, see (Saliga: column 3, lines 1-50)

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to lan dai thi truong whose telephone number is 571-272-7959. The examiner can normally be reached on monday- friday from 8:30am to 5:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, David Wiley can be reached on (571) 272-3923. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Lan Dai Thi Truong
Examiner
Art Unit 2143

Ldt
01/26/2006

DAVID WILEY
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100